

【特許請求の範囲】

【請求項1】 ネットワークに接続された外部機器を利用するデータを送信する第1の情報処理装置と、上記外部機器を管理する第2の情報処理装置と、上記ネットワーク上での課金管理を行う第3の情報処理装置とを接続してなるネットワークシステムであって、

上記第1の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第3の情報処理装置に送信した上で、上記データに上記支払情報に基づく課金情報を添付して上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、上記第1の情報処理装置から上記課金情報の添付された上記データを受信したとき、上記第3の情報処理装置に対して上記課金情報についての認証要求を行う構成にしたことを特徴とするネットワークシステム。

【請求項2】 上記第3の情報処理装置は、上記第2の情報処理装置から上記認証要求があったとき、上記支払情報に基づく認証結果情報を返信することを特徴とする請求項1に記載のネットワークシステム。

【請求項3】 上記第2の情報処理装置は、上記第3の情報処理装置から受信した認証結果情報に応じて、上記受信したデータの処分を決めることを特徴とする請求項2に記載のネットワークシステム。

【請求項4】 上記第3の情報処理装置は、上記第1の情報処理装置から上記支払情報を受信したとき、確認情報を返信することを特徴とする請求項1に記載のネットワークシステム。

【請求項5】 外部との通信を行うための通信手段と、上記通信手段を介してデータを受信するデータ取得手段と、上記データ取得手段で受信したデータに課金情報が添付されているか否かを判断する課金情報判断手段と、上記通信手段を介して上記課金情報についての認証要求を行う認証手段とを備えたことを特徴とする情報処理装置。

【請求項6】 上記認証要求により得られた認証結果に応じて、上記データ取得手段で受信した上記データの処分を決めることを特徴とする請求項5に記載の情報処理装置。

【請求項7】 上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記データに所定の処理を施すことを特徴とする請求項5に記載の情報処理装置。

【請求項8】 上記データ取得手段で受信した上記データに応じて、上記通信手段を介して外部から必要なソフトウェアを取得するソフトウェア取得手段を備えたことを特徴とする請求項5に記載の情報処理装置。

【請求項9】 上記ソフトウェア取得手段は、上記認証手段により上記認証要求を行ってから上記認証結果を得

るまでの待ち時間に上記ソフトウェアの取得を行うことを特徴とする請求項8に記載の情報処理装置。

【請求項10】 ネットワークに接続された外部機器を利用するデータを送信する第1の情報処理装置と、上記外部機器を管理する第2の情報処理装置と、上記ネットワーク上での課金管理を行う第3の情報処理装置とを接続してなるネットワークシステムであって、

上記第1の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第3の情報処理装置に送信して、上記データを上記第2の情報処理装置に送信し、

上記第3の情報処理装置は、上記第1の情報処理装置から上記支払情報を受信したとき、上記支払情報に基づく入金情報を上記第2の情報処理装置に送信し、

上記第2の情報処理装置は、上記第1の情報処理装置から上記データを受信し、上記第3の情報処理装置から上記入金情報を受信する構成にしたことを特徴とするネットワークシステム。

【請求項11】 上記第1の情報処理装置から送信される上記データと、上記第3の情報処理装置から送信される上記入金情報とは互いに対応付けられていることを特徴とする請求項10に記載のネットワークシステム。

【請求項12】 外部との通信を行うための通信手段と、

上記通信手段を介してデータを受信するデータ取得手段と、

上記通信手段を介して入金情報を受信する入金情報取得手段と、

上記データ取得手段で受信した上記データと上記入金情報取得手段で受信した上記入金情報との対応付けを確認する確認手段とを備えたことを特徴とする情報処理装置。

【請求項13】 上記データ取得手段で受信した上記データを保存する保存手段を備えたことを特徴とする請求項12に記載の情報処理装置。

【請求項14】 上記確認手段は、上記データ取得手段で受信したデータと上記入金情報取得手段で受信した入金情報との対応付けを、上記データ及び上記入金情報のそれぞれに付されたIDにより確認することを特徴とする請求項12に記載の情報処理装置。

【請求項15】 通信によりデータを受信するデータ取得手順と、

上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを有することを特徴とする情報処理方法。

【請求項16】 通信によりデータを受信するデータ取得手順と、

通信により入金情報を受信する入金情報取得手順と、上記データ取得手順で受信した上記データと上記入金情

報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを有することを特徴とする情報処理方法。

【請求項17】 通信によりデータを受信するデータ取得手順と、

上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを実行するためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【請求項18】 通信によりデータを受信するデータ取得手順と、

通信により入金情報を受信する入金情報取得手順と、上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを実行するためのプログラムを記憶したことを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークシステム、情報処理装置、情報処理方法、及びコンピュータ読み取り可能な記憶媒体に関し、特にネットワーク上の機器の管理者と利用者とは離れているものに用いて好適なものである。

【0002】

【従来の技術】一般に旧来のインターフェースは、装置間を物理的に固定接続してデータの送受を行うものであった。そのため、異なった装置とデータの送受を行う場合には、物理的に接続し直す必要があった。

【0003】データの送受信を行う装置を変更するとともに物理的な接続を変更する手間を省くようにしたのがネットワークインターフェースである。ネットワークインターフェースによれば、従来は単体で使用されていた複写機や一の装置に一对一で接続されていたプリンタ等も、より高次の使用法が可能となる。例えば、デジタル複写機の印字機構をプリンタとして使用したり、デジタル複写機のスキヤナ機構をコンピュータの画像読み取り装置として利用したりすることが可能となる。これは、複写機、プリンタ、ファクシミリ装置等の構成機構を個々に独立に扱えるようになったということであり、共通の機構を有するネットワーク接続されたこれら機器においては、運用上個々の機器の本質的差異が消失しつつある。

【0004】これに対応するように、オフィスにおけるスペースの有効活用といった市場要求等から、ファクシミリ機能、複写機能、プリンタ機能、スキヤナ機能等を一台に集積したマルチファンクションマシンが登場してきた。こうしたマルチファンクションマシンによれば、重複する機能を共通化することで、トータルのコストや

設置面積の低減を図ることが可能となる。

【0005】マルチファンクションマシンは、スモールオフィスにおいてはファクシミリ送信中にコピーが使えない等の不都合が生じることもあるが、ネットワーク環境下に複数台のマルチファンクションマシンが接続されている場合、最も効率よくハードウェアのリソースを使用することが可能となる。

【0006】かかるマルチファンクションマシンとコンピュータ等をネットワークを介して相互接続して社内ローカルエリアネットワークを構築し、さらにセキュリティを司るファイアウォールを通じて社外のインターネットへと繋ぐことも一般的となってきている。このようなシステムでは、インターネットを介して遠方から画像データを送れば、従来のファクシミリとして使用することができる。

【0007】

【発明が解決しようとする課題】上記従来例で述べたように広域ネットワークを利用する場合、機器管理者と機器利用者とは物理的に離れていることが一般的となる。

【0008】現在でも、例えば電話回線を用いたファクシミリの利用においては、印字出力に使用されて消耗品を消費する機器と、その機器を利用する者とは離れていることにより、消耗品を使用する機器の管理者に一方的に経済的負担が押しつけられるといった不都合があった。このため、いたずらファックスにより用紙が無駄に使用されてしまったり、宣伝広告を一方的に押しつけられてしまったりする等のトラブルが後を絶たなかった。

【0009】インターネット経由の情報量は従来の電話回線ファクシミリでの情報量よりも容易に膨大にすることができる。デジタル化されたデータはプログラムで生成したデータとスキヤナで読み取った画像とを区別しないことから、上記のようなトラブルの規模が大きくなってしまいが容易に予想される。

【0010】このため、インターネットと接続されたネットワーク下での不当な機器利用に対する適切な対策をとることが必要とされる。

【0011】かかる対策をとるために、ローカルネットワークを外部に繋ぐインターネット上のファイアウォールを用いることも考えられるが、ファイアウォールは情報の不正な流出を防ぐことを基本的な目的としたものであり、情報の流入に対する判断は負担が大きくなり過ぎ、かつ、ネットワークの柔軟な利用を妨げることになり、ネットワーク自体のメリットを失わせることになりかねない。したがって、他の手法により、機器管理者と機器利用者との不一致による不都合を解消するための受益者負担のシステムを構築することが必要な状況となっている。

【0012】本発明は、このような問題を解決するために成されたものであり、ネットワークの柔軟な利用を妨げることなく、受益者負担のシステムを構築することを

目的とする。

【0013】

【課題を解決するための手段】本発明は上記の課題を解決するためになされたものであり、第1に、本発明のネットワークシステムは、ネットワークに接続された外部機器を利用するデータを送信する第1の情報処理装置と、上記外部機器を管理する第2の情報処理装置と、上記ネットワーク上での課金管理を行う第3の情報処理装置とを接続してなるネットワークシステムであって、上記第1の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第3の情報処理装置に送信した上で、上記データに上記支払情報に基づく課金情報を添付して上記第2の情報処理装置に送信し、上記第2の情報処理装置は、上記第1の情報処理装置から上記課金情報の添付された上記データを受信したとき、上記第3の情報処理装置に対して上記課金情報についての認証要求を行う構成にした点に特徴を有する。

【0014】第2に、上記第3の情報処理装置は、上記第2の情報処理装置から上記認証要求があったとき、上記支払情報に基づく認証結果情報を返信する点に特徴を有する。第3に、上記第2の情報処理装置は、上記第3の情報処理装置から受信した認証結果情報に応じて、上記受信したデータの処分を決める点に特徴を有する。第4に、上記第3の情報処理装置は、上記第1の情報処理装置から上記支払情報を受信したとき、確認情報を返信する点に特徴を有する。

【0015】また、第5に、本発明の情報処理装置は、外部との通信を行うための通信手段と、上記通信手段を介してデータを受信するデータ取得手段と、上記データ取得手段で受信したデータに課金情報が添付されているか否かを判断する課金情報判断手段と、上記通信手段を介して上記課金情報についての認証要求を行う認証手段とを備えた点に特徴を有する。

【0016】第6に、上記認証要求により得られた認証結果に応じて、上記データ取得手段で受信した上記データの処分を決める点に特徴を有する。第7に、上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記データに所定の処理を施す点に特徴を有する。第8に、上記データ取得手段で受信した上記データに応じて、上記通信手段を介して外部から必要なソフトウェアを取得するソフトウェア取得手段を備えた点に特徴を有する。第9に、上記ソフトウェア取得手段は、上記認証手段により上記認証要求を行ってから上記認証結果を得るまでの待ち時間に上記ソフトウェアの取得を行う点に特徴を有する。

【0017】また、第10に、本発明のネットワークシステムは、ネットワークに接続された外部機器を利用するデータを送信する第1の情報処理装置と、上記外部機器を管理する第2の情報処理装置と、上記ネットワーク上での課金管理を行う第3の情報処理装置とを接続して

なるネットワークシステムであって、上記第1の情報処理装置は、上記外部機器を利用するとき、料金支払いに関する支払情報を上記第3の情報処理装置に送信して、上記データを上記第2の情報処理装置に送信し、上記第3の情報処理装置は、上記第1の情報処理装置から上記支払情報を受信したとき、上記支払情報に基づく入金情報を上記第2の情報処理装置に送信し、上記第2の情報処理装置は、上記第1の情報処理装置から上記データを受信し、上記第3の情報処理装置から上記入金情報を受信する構成にした点に特徴を有する。

【0018】第11に、上記第1の情報処理装置から送信される上記データと、上記第3の情報処理装置から送信される上記入金情報とは互に対応付けられている点に特徴を有する。

【0019】また、第12に、本発明の情報処理装置は、外部との通信を行うための通信手段と、上記通信手段を介してデータを受信するデータ取得手段と、上記通信手段を介して入金情報を受信する入金情報取得手段と、上記データ取得手段で受信した上記データと上記入金情報取得手段で受信した上記入金情報との対応付けを確認する確認手段とを備えた点に特徴を有する。

【0020】第13に、上記データ取得手段で受信した上記データを保存する保存手段を備えた点に特徴を有する。第14に、上記確認手段は、上記データ取得手段で受信したデータと上記入金情報取得手段で受信した入金情報との対応付けを、上記データ及び上記入金情報のそれぞれに付されたIDにより確認する点に特徴を有する。

【0021】また、第15に、本発明の情報処理方法は、通信によりデータを受信するデータ取得手順と、上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを有する点に特徴を有する。

【0022】第16に、本発明の情報処理方法は、通信によりデータを受信するデータ取得手順と、通信により入金情報を受信する入金情報取得手順と、上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを有する点に特徴を有する。

【0023】また、第17に、本発明のコンピュータ読み取り可能な記憶媒体は、通信によりデータを受信するデータ取得手順と、上記データ取得手順で受信した上記データに課金情報が添付されているか否かを判断する課金情報判断手順と、通信により上記課金情報についての認証要求を行う認証手順とを実行するためのプログラムを記憶した点に特徴を有する。

【0024】第18に、本発明のコンピュータ読み取り可能な記憶媒体は、通信によりデータを受信するデータ取得手順と、通信により入金情報を受信する入金情報取

得手順と、上記データ取得手順で受信した上記データと上記入金情報取得手順で受信した上記入金情報との対応付けを確認する確認手順とを実行するためのプログラムを記憶した点に特徴を有する。

【0025】上記のようにした本発明では、外部から受信したデータに課金情報が添付されていなかったり、課金情報が正当なものでなかったりした場合、又は、外部から受信したデータに対応する入金情報がない場合に、機器を利用させない等の処分を行うことが可能となり、不当な機器利用に対する適切な対策をとることができる。

【0026】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

(第1の実施の形態)図1には、第1の実施の形態のネットワークシステムの概要を示す。このネットワークシステムでは、外部機器4を利用するデータを送信する機器利用者側の情報処理装置1と、上記外部機器4を管理する機器管理者側の情報処理装置2と、ネットワーク上での課金管理を行う情報処理装置3とを具備し、インターネット等の通信網を介して互いに接続している。

【0027】機器利用者側の情報処理装置1は、通信網に接続するための通信部11と、情報処理装置3に支払情報を送信する支払情報発生部12と、情報処理装置3から確認情報を受信する確認情報取得部13と、機器管理者側の情報処理装置2に上記支払情報に基づく課金情報を添付したデータを送信するデータ出力部14とを有する。

【0028】機器管理者側の情報処理装置2は、通信網に接続するための通信部21と、機器利用者側の情報処理装置1からデータを受信するデータ取得部22と、データ取得部22で受信したデータに機器4を利用するための処理を施すデータ処理部23と、データ取得部22で受信したデータに課金情報が添付されている否かを判断する課金情報判断部24と、情報処理装置3に課金情報についての認証要求を行う認証部25とを有する。なお、この情報処理装置2は、機器4と別に設けられたものであってもよいし、機器4に内蔵されたものであってもよい。

【0029】課金管理用の情報処理装置3は、通信網に接続するための通信部31と、機器利用者側の情報処理装置1から支払情報を受信する支払情報取得部32と、支払情報についての確認情報を返信する確認情報発生部33と、機器管理者側の情報処理装置2から認証要求があったとき認証結果情報を返信する認証情報発生部34とを有する。この課金管理用の情報処理装置3としては、後からも述べるが、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う電子マネーサーバ等が用いられる。

【0030】例えば、機器利用者は、画像データを送っ

て外部機器4を利用しようとする場合、まず課金管理用の情報処理装置3に支払情報を送信する(図中矢印A1)。支払情報は、機器管理者への料金支払いに関する情報であり、自己の保有する金額からいくら支払うかの情報(支払い額情報)が含まれる。この支払情報は、第三者への漏洩を防止するために暗号化する等して情報処理装置3に送信される。

【0031】課金管理用の情報処理装置3は、上記支払情報を受信したならば、確認のための確認情報を機器利用者側の情報処理装置1に送信する(図中矢印A2)。なお、支払情報は暗号化されているので情報処理装置3側での解読用の鍵が必要となるが、これは銀行の口座でいえば出金時の暗証番号に相当する。

【0032】機器利用者側の情報処理装置1は、課金管理用の情報処理装置3から確認情報を受信したならば、上記支払情報に基づく課金情報を添付した画像データを機器管理者側の情報処理装置2に送信する(図中矢印A3)。この課金情報とは、必要な額の支払い能力があり、機器管理者に対して料金を支払う意志があることを示すもので、少なくとも、料金を支払う者(機器利用者)、料金を受け取る者(機器管理者)、支払い金額の3項目を含んでいる。これら全ての情報も、第三者への漏洩を防止するよう保護されていなければならない。また、ネットワーク上には課金管理用の情報処理装置3が1つだけとは限らず、課金情報の認証先を特定する必要があることから、当該課金情報には、どこに問い合わせるかについての情報も含まれている。

【0033】機器管理者側の情報処理装置2では、機器利用者側から課金情報の添付された画像データを受信したならば、課金管理用の情報処理装置3に対してその課金情報についての認証要求を行う(図中矢印A4)。

【0034】課金管理用の情報処理装置3では、機器管理者側からの認証要求があったならば、事前に機器利用者側から支払情報のあったものかどうかを確認し、正当なものか否かの認証を行うべく機器管理者側の情報処理装置2に認証結果情報を送信する(図中矢印A5)。

【0035】機器管理者側の情報処理装置2では、課金情報が正当なものであるとの認証情報を得た場合は、機器4の利用を許可する。それに対して、課金情報が添付されていなかったり、課金情報が正当なものでなかったりした場合は、機器4を利用させない等の処分を行うことで、不当な機器利用に対する適切な対策をとることができる。

【0036】なお、機器利用者が課金管理用の情報処理装置3に課金情報と画像データとを送信し、それを機器管理者側の情報処理装置2に転送してもらうといった手法も考えられる。しかし、画像データが長大な情報量となることもあり、このような画像データが課金情報とともに送信されてくると、課金管理用の情報処理装置3の負担が増大し過ぎることも予想される。そこで、本実施

の形態では、上述のように、機器利用者側の情報処理装置1は、課金管理用の情報処理装置3に支払情報のみを送信した上で、機器管理者側の情報処理装置2に課金情報を添付した画像データを直接送信するようにしている。

【0037】ここまで述べた課金管理はいわゆる預金方式によるが、課金管理用の情報処理装置3への事前の支払い額確認を簡略化したクレジットカード方式をとることも可能である。この場合は、機器利用者側から課金管理用の情報処理装置3へ事前に支払情報を送る必要がないが、機器管理者側からの不当な金額要求等のトラブルに対応できないので、支払額に限度を設定する等の現行のクレジットカードで実施されているような対策が必要となる。

【0038】図2は、ネットワークシステムの一具体例を示す図である。100はインターネット等の通信網である。200はウェブサーバであり、インターネットユーザに特定のサービスを提供する。

【0039】300は電子マネーサーバであり、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う。400はサービスプロバイダであり、個人ユーザの端末とインターネット100との接続処理を行う。500はファイアウォールであり、LANと外部通信網であるインターネット100とを接続し、セキュリティ管理等を行う。

【0040】LANにおいて、600は機器管理サーバであり、LAN上に接続された各機器700~1000の管理、ユーザ管理、課金情報等のデータ管理等を行う。700はファイルサーバであり、広告データの管理等を行う。800はマルチファンクションマシンであり、詳しくは後述するが、主に画像データの入出力等の機能を有する。

【0041】900はプリンタであり、パーソナルコンピュータ1000やファイルサーバ700からの画像データを記録媒体上にプリントする。1000は端末装置として接続されたパーソナルコンピュータであり、インターネット100を介してウェブサーバ200から提供された情報を閲覧したり、画像データをマルチファンクションマシン800やプリンタ900に出力したりする。なお、上記マルチファンクションマシン800やプリンタ900が、図1で説明した機器4に相当するものである。

【0042】上記マルチファンクションマシン800は、ユーザが操作するための操作部810、操作部810やパーソナルコンピュータ1000からの指示に従って画像を入力するためのイメージスキャナ820、パーソナルコンピュータ1000やファイルサーバ700からのデータを印刷するプリンタ830、デバイスコントローラ840、メモリ850、ハードディスク860から構成される。

【0043】このようにしたマルチファンクションマシン800において、上記デバイスコントローラ840は、操作部810やパーソナルコンピュータ1000からの指示に従って、イメージスキャナ820、プリンタ830、メモリ850やハードディスク860、パーソナルコンピュータ1000の間で画像データの入出力等の制御を行う。例えば、イメージスキャナ820により読み込んだ画像データをメモリ850やハードディスク860に必要な応じて蓄積したり、パーソナルコンピュータ1000に出力したり、あるいはプリンタ830で印刷したりする等の制御を行う。このデバイスコントローラ840は、ハードウェアの描画機構及びCPUと実行ソフトウェアによって構成される。

【0044】なお、図面上においてファイアウォール500より下方に示したLAN構成は、サービスプロバイダ400を介してインターネットに繋がっている個人ユーザのもとにあってもよい。

【0045】次に、インターネット経由で、遠方のユーザからファクシミリ情報又は印字出力要求を伴うイメージ情報（以下、データという）がLANに送られてきたときの動作を説明する。

【0046】遠方のユーザは、マルチファンクションマシン800やプリンタ900を正当な課金負担の下で意図する出力を実行して利用するのであれば、既に説明したように、送信するデータに適切な課金情報を添付する。

【0047】以下、図3のフローチャートを用いて、遠方のユーザからデータが送られてきたときのマルチファンクションマシン800やプリンタ900側での処理を説明する。ステップS101で、インターネット等の通信網100を経由したデータ（データパケット）を受信したならば、ステップS102で、そのデータに課金情報が添付されているか否かを確認する。

【0048】ステップS102において課金情報が添付されていれば、ステップS103で認証パケットを送出し、電子マネーサーバ300に対して当該課金情報についての認証要求を行う。また、ステップS104でデータ処理を開始して出力イメージを生成し、ステップS105で出力イメージを生成した状態で電子マネーサーバ300からの認証を待機する。

【0049】そして、電子マネーサーバ300から認証結果情報の返信があったならば、ステップS106で上記課金情報が正当なものであるか否かを判定し、正当なものであれば、既に生成した出力イメージについて印字出力を実行する（ステップS107）。すなわち、正当な課金情報を添付してきたユーザに対しては機器を利用させることとなる。ステップS106の判定において課金情報が正当なものでないと判定された場合は、後述するステップS112に移る。

【0050】なお、課金情報についての認証を行う際

に、情報隠蔽手段が用意されていないインターネット等のネットワーク上に情報を流すのは問題がある。したがって、課金情報の認証には、十分な暗号化を施すか、あるいは専用線を使用することによって実施するのが望ましい。ローカルネットワークを課金情報のために二重化するのが現実的でない場合は、ファイアウォール500内は暗号化によって、電子マネーサーバ300までは専用線を使用することによって等の運用上の使い分けを行えばよい。

【0051】一方、上記ステップS102において課金情報が添付されていなければ、ステップS108でユーザ情報確認パケットを送出し、ローカルサーバ（機器管理サーバ600）に機器利用者に関するユーザ情報を確認する。また、ステップS109でデータ処理を開始してイメージ出力を生成し、ステップS110で出力イメージを生成した状態でローカルサーバからのユーザ情報を待機する。

【0052】そして、ローカルサーバからユーザ情報が送られてきたら、ステップS111で、データの送信元が信用に値するとして登録されているユーザであるかどうかを判定する。信用に値するとして登録されているとのユーザ情報が得られれば、ステップS107に移って、既に生成した出力イメージについて印字出力を行う。すなわち、データに課金情報が添付されていなかった場合でも、特定のユーザに対しては機器を利用させることとなる。ステップS111の判定において登録もされていないユーザであるとのユーザ情報が得られた場合は、後述するステップS112に移る。

【0053】ステップS112、S113では、正当でない課金情報が添付されていたデータ（ステップS106）、あるいは、課金情報が添付されずユーザ登録もないデータ（ステップS111）についての処分が決定される。本実施の形態では、仮出力モード、情報保存モード、破棄モードといった3つのモードが設定され、機器管理者側の設定に応じていずれかのモードが選択される。

【0054】仮出力モードに設定されていた場合、正当でない課金情報が添付されていたデータ、あるいは、課金情報が添付されずユーザ登録もないデータについても印字出力を行う（ステップS114～S116）。ただし、ステップS115で出力用紙を切り替えて廉価な用紙を選択した上で、ステップS116で印字出力を行うようにしている。そのため、ステップS114においては、既に生成されている出力イメージのリサンプル、変換処理を行っている。なお、廉価な用紙を使用する以外にも、縮小印刷とする、省トナー印字を行う、カラー印刷をモノクロで代用する等の廉価な印字モードにより出力を行うようにしてもよい。

【0055】また、情報保存モードに設定されていた場合、既に生成されている出力イメージを、マルチファク

ションマシン800やプリンタ900、外部のパーソナルコンピュータ1000、機器管理サーバ600等に転送して保存する（ステップS117）。これにより、機器管理者は、データの内容を確認した上で、印字出力するか、あるいは、データを破棄するかを判断することが可能となる。

【0056】また、破棄モードに設定されている場合、既に生成されている出力イメージを破棄する（ステップS118）。つまり、正当でない課金情報が添付されていたデータ、あるいは、課金情報が添付されずユーザ登録もないデータについては、印字出力を一切拒否することになる。

【0057】以上述べた第1の実施の形態によれば、正当な料金を支払うユーザには機器を利用させるとともに、不当な利用に対しては適当なデータの処分を行うことで、機器管理者が経済的不利益をこうむることのない受益者負担のシステムを構築することができる。

【0058】（第2の実施の形態）多くの入出力機構を備えるマルチファンクションマシンにおいては、要求される画像処理パターンは多岐にわたり、扱うデータフォーマットも多くなる。これら全てに対応するプログラムを単体の実装、製品化することには、かなりのコストが見込まれる。また、新規フォーマット、新規の画像処理処理パターンに対するアップデート作業も大変なものとなる。

【0059】ネットワークに接続されることを前提とするマルチファンクションマシンにおいては、必要最小限の機能のみを実装し、必要なソフトウェアはその都度サーバ等から取得し、実行するという機器構成をとるといった選択肢がある。このような機器構成によるメリットは、マルチファンクションマシン単体の記憶容量等のコストを下げることができ、また、ソフトウェアのアップデートも容易となることである。さらに、ソフトウェアのアップデートが容易であることによって、個別機器の物理的リプレイスなしで新規に設定されたデータフォーマットにも対応が可能となる。

【0060】なお、デメリットとしては、ネットワークやサーバにトラブルが発生し情報のやり取りができなくなった場合に、単体では多くの処理が行えなくなることが挙げられる。しかし、もともとネットワークやサーバにトラブルが発生した場合は、マルチファンクションマシンのプリンタやファクシミリとしての使用は不可能となることから、多くの機能において上記のデメリットは無視しうるものといえる。

【0061】そこで、本実施の形態では、ネットワーク間の情報の入出力を主体としたマルチファンクションマシンにおいては、必要なソフトウェアはその都度サーバ等から取得し、実行するという機器構成をとることにしている。

【0062】ここで、上記第1の実施の形態で述べたよ

うに、機器管理者側では、課金情報の正当性を確認するために、電子マネーサーバ300との間で認証のやり取りを行わなければならない。図2でいえば、LAN内部とLAN外部との情報のやり取りを行う必要があることから、タイムラグが生じ、認証結果情報を得るまでの待ち時間ができる公算が大きい。

【0063】そこで、本実施の形態では、この待ち時間を、ローカルサーバからの必要なアプリケーションのダウンロード時間として利用することにしている。以下、図4のフローチャートを用いて、第2の実施の形態での処理を説明する。なお、本第2の実施の形態の構成としては、データの受信機構、課金情報の確認機構をデフォルトとして個別機器に格納する。

【0064】ステップS201で、インターネット等の通信網100を経由したデータ（データパケット）を受信したならば、ステップS202で認証パケットを送出し、電子マネーサーバ300に対して当該課金情報についての認証要求を行う。

【0065】また、ステップS203で受信したデータのデータフォーマットを解析し、ステップS204で、内蔵するプログラムによるデータ処理が可能か否かを判断する。

【0066】上記ステップS204において対応する内蔵プログラムでの処理ができないと判断されたならば、ステップS205で、ローカルサーバに対して必要なアプリケーションの転送を要求する。そして、アプリケーションの転送を待って（ステップS206）、転送が終了したならば（ステップS207）、ステップS208でデータ処理を開始して出力イメージを生成し、ステップS209で出力イメージを生成した状態で電子マネーサーバ300からの認証を待機する。

【0067】そして、電子マネーサーバ300から認証結果情報の返信があったならば、ステップS210で上記課金情報が正当なものであるか否かを判定し、正当なものであれば、既に生成した出力イメージについて印字出力を行う（ステップS211）。

【0068】なお、上記ステップS204において対応する内蔵プログラムがあると判断されれば、ソフトウェアをダウンロードする必要はないので、そのままステップS208に移る。

【0069】アプリケーションの転送が規定時間を超えてもなされない場合（ステップS212）や、課金情報が正当なものでないとの認証結果が得られた場合（ステップS210）、ステップS213に移って例外処理を行う。

【0070】以上説明した図4においては、表記上フローチャートとして記述しているが、電子マネーサーバ300からの認証待ちと、アプリケーションの受信及びデータ処理とは並列に実行される必要がある。そして、実際にどちらかを「待つ」のは、いずれか一方の処理が全

て終わった時点での話である。例えば、データ処理の終了前に課金情報が正当である旨の認証結果を得た場合、そのデータ処理を継続する。データ処理の終了前に課金情報が正当でない旨の認証結果を得た場合は、データ処理をその時点でキャンセルする。

【0071】アプリケーションとしては、例えばデータフォーマットが付加されている使用要求に対しては、データフォーマットごとにアプリケーションもしくはアプリケーションのモジュールを用意してもよい。この場合、データフォーマットをローカルサーバに通知し、対応するアプリケーションやモジュール等を受け取り実行する。

【0072】（第3の実施の形態）上記第1の実施の形態では、図1に示す矢印A1～A5で説明したような手順をとるようにしたが、機器利用者は課金管理用の情報処理装置3からの確認情報を待つ必要がある（図中矢印A2）、また、機器管理者は課金管理用の情報処理装置3に認証要求を行って認証を待機する必要があることから（図中矢印A4、A5）、待ち時間が生じてしまう。

【0073】そこで、本第3の実施の形態では、図5に示すようにして情報のやり取りを行うようにしている。

【0074】機器利用者側の情報処理装置1は、通信網に接続するための通信部15と、情報処理装置3に支払情報を送信する支払情報発生部16と、機器管理者側の情報処理装置2にIDを付したデータを送信するデータ出力部17とを有する。

【0075】機器管理者側の情報処理装置2は、通信網に接続するための通信部26と、機器利用者側の情報処理装置1からデータを受信するデータ取得部27と、データ取得部27で受信したデータに機器4を利用するための処理を施すデータ処理部28と、課金管理用の情報処理装置3から入金情報を受信する入金情報取得部29と、上記入金情報に付されたIDと上記データに付されたIDとの対応付けを確認するID確認部30とを有する。

【0076】課金管理用の情報処理装置3は、通信網に接続するための通信部35と、機器利用者側の情報処理装置1から支払情報を受信する支払情報取得部36と、機器管理者側の情報処理装置2に入金情報を送信する入金情報発生部37とを有する。上記入金情報は、支払情報取得部36で受信した支払情報に基づくもので、IDが付された状態で機器管理者側の情報処理装置2に送信される。この課金管理用の情報処理装置3としては、前述のように、銀行等の金融機関と消費者クライアントとの間の決済処理等を行う電子マネーサーバ等が用いられる。

【0077】例えば、機器利用者は、画像データを送って外部機器4を利用しようとする場合、まず機器管理用の情報処理装置3に支払情報を送信する（図中矢印B1）。支払情報は、機器管理者への料金支払いに関する

情報であり、自己の保有する金額からいくら支払うかの情報（支払い額情報）が含まれる。

【0078】また、機器利用者は、機器管理者側の情報処理装置2に、所定のIDを含ませた画像データを送信する（図中矢印B2）。

【0079】課金管理用の情報処理装置3は、上記支払情報を受信したならば、その支払情報に基づく入金情報を機器管理者側の情報処理装置2に送信する（図中矢印B3）。この入金情報は、機器利用者側からの支払いがある旨を伝える情報であり、所定のIDを含ませた状態で送信される。

【0080】機器管理者側の情報処理装置2は、機器利用者側から画像データを受信し、また、課金管理用の情報処理装置3から入金情報を受信したならば、これら画像データ及び入金情報に付されているIDを確認して、互いに対応するものかどうかを判断する。そして、画像データと入金情報とが対応するものであれば、機器4の利用を許可する。それに対して、画像データに対応する入金情報の受信がないような場合は、機器4を利用させない等の処分を行うことで、不当な機器利用に対する適切な対策をとることができる。

【0081】この第3の実施の形態でも、図2に示したネットワークシステムに基づいて、インターネットを経由したデータ及び入金情報がLANに送られてきたときの動作を説明する。図6は、データ及び入金情報が送られてきたときのマルチファンクションマシン800やプリンタ900側での処理を説明するためのフローチャートである。本実施の形態では、マルチファンクションマシン800やプリンタ900側に入金情報とデータとが別々に送られてくるので、2つの独立したフローチャートにより処理が行われる。

【0082】図6（a）は、データを受信したときの処理を示す。ステップS301で、インターネット等の通信網100を経由したデータ（データパケット）を受信したならば、ステップS302でデータ処理を開始し、ステップS303で出力イメージを生成する。

【0083】そして、ローカルサーバ（機器管理サーバ600）に機器利用者に関するユーザ情報を確認し、ステップS304で、データの送信元が信用に値するとして登録されているユーザであるかどうかを判定する。

【0084】信用に値するとして登録されているとのユーザ情報が得られれば、ステップS304に移って、既に生成した出力イメージについて印字出力を行う。すなわち、特定のユーザに対しては、データが送られてきた時点で機器を利用させる。

【0085】登録もされていないユーザであるとのユーザ情報が得られた場合は、ステップS306に移って、出力イメージをハードディスク860に保存しておく。データと入金情報とは別々に送られてくることから、データに遅れて入金情報が送られてくることも多く、その

場合に、入金情報の遅れで重要な情報が破棄されるのを防ぐためである。

【0086】図6（b）は、入金情報を受信したときの処理を示す。インターネット等の通信網100を経由して入金情報を受信したならば、ステップS307で、ハードディスク860に保存されたイメージ出力（図6（a）のステップS306）の順次読み出しを開始する。そして、ステップS308で、保存されているイメージ出力があるかどうかを判定する。

【0087】保存されているイメージ出力がある場合、ステップS309に移って、そのイメージ出力についてのID（データに付されていたID）を、入金情報に付されたIDと比較する。そして、両IDが一致するものであれば（ステップS310）、すなわち、データと入金情報とが対応するものであれば、ステップS311で当該出力イメージについて印字出力を行う。印字出力の終了した出力イメージはハードディスク860から消去して破棄する（ステップS312）。なお、両IDが一致しなければ（ステップS310）、順次別データを読み出すようにして（ステップS313）、入金情報に対応する出力イメージを探し出す。

【0088】ステップS308においてイメージ出力がなければ、ステップS314に移って、入金情報に対応するデータがないとして終了する。

【0089】図7のフローチャートには、データのみが送信されて入金情報がない場合に、ハードディスク860に保存されている当該データの出力イメージを破棄するための処理を示す。

【0090】図6（a）で述べたように、受信したデータの出力イメージをハードディスク860に保存して入金情報の受信を待機するが、ある程度の時間が経っても未だ入金情報が送られてこない場合は、不当に機器を利用しようとするものと考えられる。この場合には、ハードディスク860の空き容量を確保するためにも、不要な情報を削除する必要がある。なお、このフローチャートは、例えば1日に1回、日付の変化に合わせて起動するようにしておけばよい。

【0091】ステップS315では、ハードディスク860に保存されているイメージ出力の順次読み出しを開始する。そして、ステップS316で、保存されているイメージ出力があるかどうかを判定する。

【0092】保存されているイメージ出力がある場合、ステップS317でその登録日時を確認し、ステップS318では、保存されてから現在までの時間が予め設定されている規定時間を超過しているか否かを判断する。

【0093】そして、規定時間を超過していれば、対応する入金情報の受信はもうないものと考えられるので、ステップS319に移って、そのイメージ出力を不要なものとしてハードディスク860から削除する。

【0094】このようにしてハードディスク860に保

存されている全ての出力イメージについて判断して（ステップS320）、このフローチャートを終了する。

【0095】以上述べた第3の実施の形態によれば、機器管理用の情報処理装置3（電子マネーサーバ300）から機器管理者側に直接に入金情報を送るようにしたので、機器利用者は確認情報を待つ必要がなく、また、機器管理者は認証要求を行い認証結果を待つ必要がなくなり、ネットワーク上のトラフィック及び待ち時間を解消することができる。

【0096】（その他の実施の形態）本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても1つの機器（例えば、複写機、ファクシミリ装置）からなる装置に適用してもよい。

【0097】また、上述した実施の形態の機能を実現するべく各種のデバイスを動作させるように、該各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（CPUあるいはMPU）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【0098】また、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0099】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【0100】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【0101】なお、上記実施の形態において示した各部

の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0102】

【発明の効果】以上説明したように本発明によれば、正当な料金を支払うユーザには機器を利用させるとともに、不当な利用に対してはデータに適当な処分を行うことで、機器管理者が経済的不利益をこうむることのない受益者負担のシステムを構築することができる。

【図面の簡単な説明】

【図1】第1の実施の形態のネットワークシステムを示す概要図である。

【図2】ネットワークシステム的具体例を示す図である。

【図3】第1の実施の形態においてインターネットを経由してデータが送信されてきたときの処理を示すフローチャートである。

【図4】第2の実施の形態での処理を説明するためのフローチャートである。

【図5】第3の実施の形態のネットワークシステムを示す概要図である。

【図6】第3の実施の形態においてインターネットを経由してデータ及び入金情報が送信されてきたときの処理を示すフローチャートである。

【図7】データのみが送信されて入金情報がない場合に、保存されている当該データの出力イメージを破棄するための処理を示すフローチャートである。

【符号の説明】

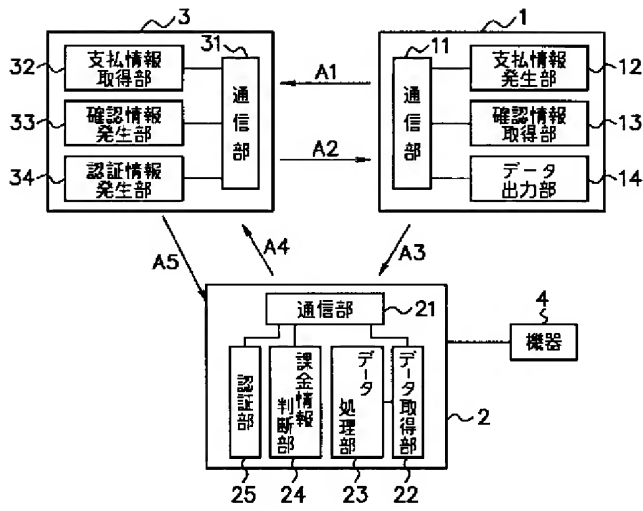
1	機器利用者側の情報処理装置
2	機器管理者側の情報処理装置
3	課金管理用の情報処理装置
4	外部機器
11、15	通信部
12、16	支払情報発生部
13	確認情報取得部
14、17	データ出力部
21、26	通信部
22、27	データ取得部
23、28	データ処理部
24	課金情報判断部
25	認証部
29	入金情報取得部
30	ID確認部
31、35	通信部
32、36	支払情報取得部
33	確認情報発生部
34	認証情報発生部

37	入金情報発生部
100	インターネット等の通信網
200	ウェブサーバ
300	電子マネーサーバ
400	サービスプロバイダ
500	ファイアウォール
600	機器管理サーバ
700	ファイルサーバ
800	マルチファンクションマシン

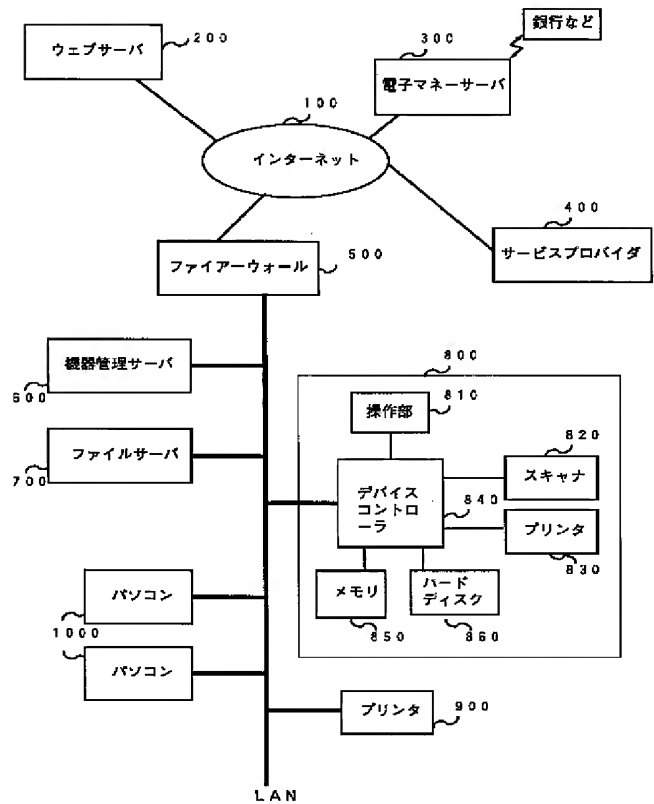
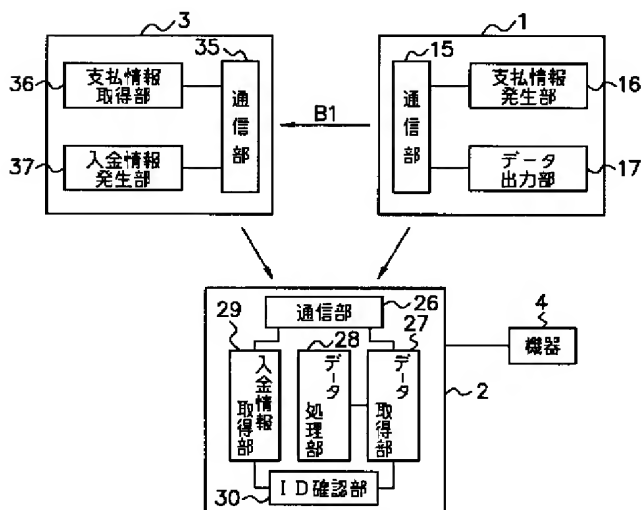
900	プリンタ
1000	パーソナルコンピュータ
810	操作部
820	イメージスキャナ
830	プリンタ
840	デバイスコントローラ
850	メモリ
860	ハードディスク

【図1】

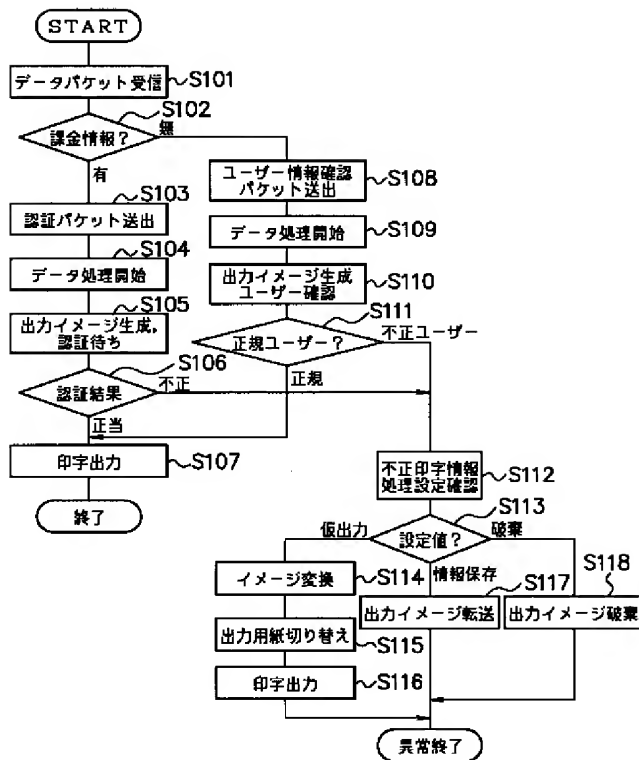
【図2】



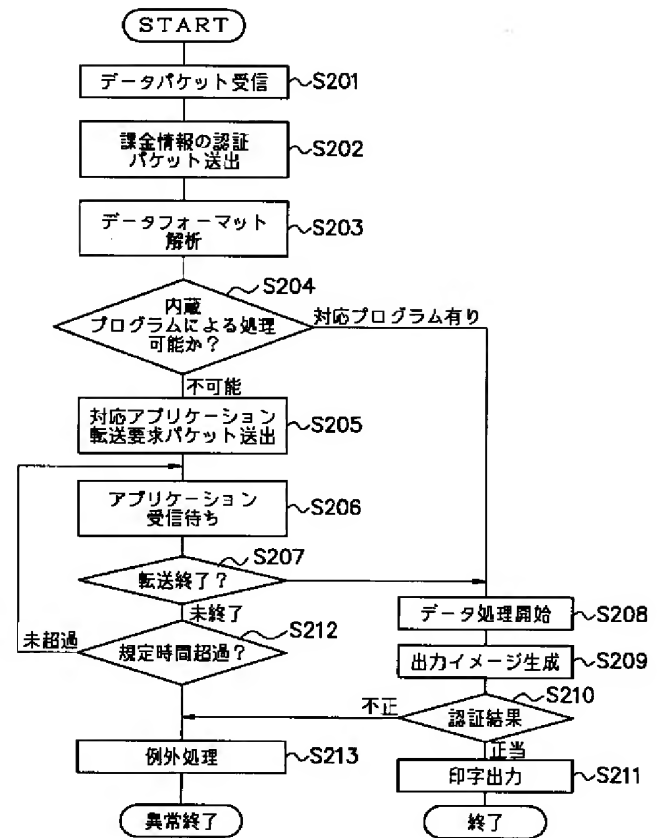
【図5】



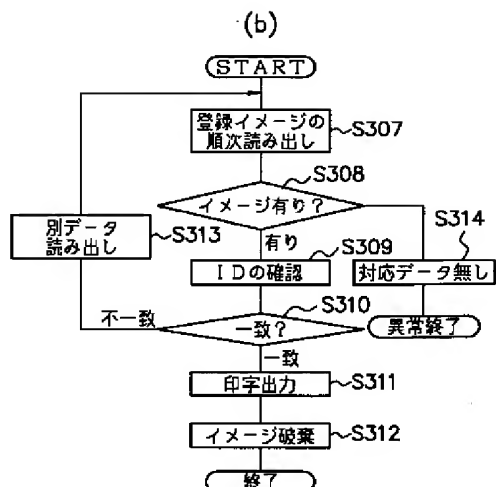
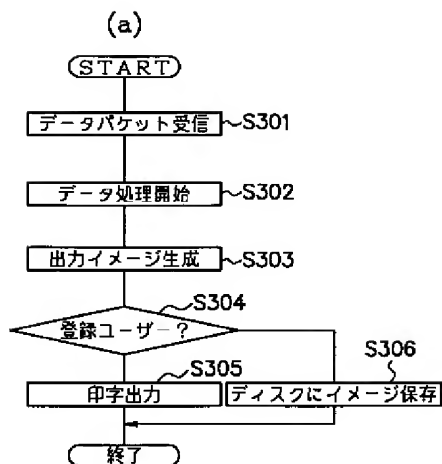
【図3】



【図4】



【図6】



【図7】

